СТАТИИ

Почитување на основните човекови права во борбата против тероризмот

Доц. д-р Олга Кошевалиска*

UDC: 323.285:343.285.02]:341.231.14:343.131.7 (4-672 ЕУ)
1.01 Изворна научна статија

Вовед

Во борбата против тероризмот и организираниот криминал како нужна се наметнува потребата од жртвување на одредени загарантирани човекови права. Во таа смисла, борбата против овие закани за националната безбедност секогаш оди на „сметка" на правото на заштита на личните податоци и правото на приватност. За успешна борба против тероризмот и организираниот криминал неопходен е пренос на лични податоци од многу извори. На овој пренос му следат снимање, толкување и ставање во корелација на податоците кои се добиени. Информатичката фузија на овие податоци како и дополнувањето на делумните информации беше особен предизвик за повеќето држави во рамките на Европската Унија (во понатамошниот текст ЕУ) (Committee on Science and Technology for Countering Terrorism, National Research Council: Washington, D.C.). Со оглед на фактот дека ЕУ најмногу се има концентрирано на превенцијата на тероризмот, преносот, собирањето, задржувањето и обработката на личните податоци е од неизмерна важност. Од друга страна пак, ова сериозно се коси со правото на заштита на лични податоци како и со останатите основни човекови права меѓу кои ќе го издвоиме правото на презумпцијата на невиност. Последново е од причини што како субјект на истрага се јавуваат лица кои се потполно невини, а се во некаква врска со осомничени лица (Eijkman, Q., Schuurman, B. 2011, стр.11).

Лисабонскиот договор доведе до унапредување на инструментите на Унијата во ова поле, со оглед на фактот дека истиот требаше да даде поттик во создавањето, проширувањето и одржувањето на пристапот до датабазите кои содржат екстензивни биографски и биометриски податоци, од страна на државните органи. Со овој пристап се овозможи идентификување индивидуи кои претставуваат ризик за безбедноста на државите и Унијата. Најголема заслуга на ова е можноста за аналитичка обработка на податоците и создавање профил за можни терористи, што треба да резултира со исполнување на целта – превентивно дејствување односно идентификување на терористот пред да го стори планираното дело.

Националната безбедност претставува највисоко рангирана вредност во секоја држава. Истата претставува предуслов за стабилност, правилно функционирање и континуитет во постоењето на државата. Таа е од витално значење за националната и индивидуалната сигурност на државата. Иако државата треба да ги штити своите државјани од каква било злоупотреба на нивните права (особено фундаменталните кои се неприкосновани), сепак честа се случаите кога и самата држава си дозволува упад во основните човекови права штитејќи ја националната безбедност. Пред појавата на супранационалните и меѓународните организации кои денес се најголеми поборници за почитување на основните човекови права, државата беше единствениот гарант по ова прашање, што резултираше со обезбедување на националната безбедност на сметка на индивидуалната сигурност. Несомнено е дека постои едно екстензивно преклопување во областа на човекови права и областа на националната безбедност од друга страна. Ова е и логично со оглед на фактот дека овие две области меѓусебно се дополнуваат. Според некои автори (Tadjbakhsh, S., Chenoy, A. 2007, стр.123), човековите права ја дефинираат човековата безбедност. Сржта на човековата безбедност е во почитување на човековите права и фундаменталните слободи односно „придржувањето кон човековите права е единствениот начин за постигнување на индивидуалната, националната и меѓународната безбедност". Погрешно е сфаќањето дека концептите на „национална безбедност" и „човекови права" се исклучуваат меѓусебно и не можат да коегзистираат

* Авторката е доцент на Правниот факултет во Штип, Универзитет „Гоце Делчев" од Штип.

заедно. Човековите права ја зајакнуваат безбедноста на нацијата, па оттука во интерес на државата е да ги штити истите. Бенџамин Франклин има наведено дека „оние што ќе се одречат од нивните основни права и слободи за да ја зголемат својата безбедност, не ги заслужуваат ниту правата ниту безбедноста".[1]

Правото на приватност се однесува на правото на личноста на приватен живот, без мониторинг, без разлика дали ваквиот живот вклучува односи со други личности или не, додека правото на заштита на личните податоци ги заштитува овие податоци како и сите други податоци, без разлика дали се лични или не под услов да се во врска со идентификацијата на личност. Личните податоци не мора секогаш да се поврзани со правото на приватност бидејќи самиот концепт на лични податоци е многу поширок од концептот на приватен живот. Оттука и нивното издојување во две автономни права.[2] Истиот концепт е содржан и во членот за заштита на лични податоци од Конвенцијата за заштита на лични податоци. За да постои правна сигурност во почитувањето на ова право на приватност и правото на заштита на лични податоци, како и да постои правилната заштита од какви било повреди на овие права тие мора да бидат дефинирани и определени јасно, односно да даваат јасни насоки за околностите и контролираните услови во кои државните авторитети можат да преземаат мерки со кои ќе ги дерогираат при што најважно е ваквата дерогација да е јасно определена и да не бара дополнителни правни анализи (Busser, Els, 2009 стр.5)

Институционална рамка на ЕУ за обработка на лични податоци во борбата против тероризмот

Во рамките на ЕУ, постојат повеќе тела кои што се поврзани со собирањето, обработката, задржувањето и преносот на лични податоци. ЕУРОПОЛ е прв пример за такво тело со оглед на фактот дека неговата крајна цел е соработката и кординацијата меѓу државите членки и нивните надлежни органи за постигнување на ефективна борба против транснационалниот организиран криминал и тероризмот. Компјутерскиот информативен систем на ЕУРОПОЛ (Кошевалиска, О. Нанев, Л. 2014) содржи екстензивни лични податоци за лица што покренува многу прашања во однос на заштитата на основните човекови права (правото на заштита на лични податоци, правото на приватност и правото на презумпција на невиност). Заштитата на овие права се доведува во прашање со намерата на ЕУРОПОЛ во иднина својата датабаза да ја интегрира со сличните датабази на другите тела на Унијата. Под чадорот на борба против тероризмот, ЕУРОПОЛ и разузнавачките служби од САД ја започнаа соработката (Pop, V. 2013). Друга база на податоци за непожелни лица во ЕУ припаѓа на Frontex, Агенција за надворешните граници на Унијата чијашто задача е заштита на надворешните граници на Унијата примарно од илегални мигранти. Оваа агенција, во бробата против тероризмот се стреми кон поширкоа дата база на биометриски податоци, сателитски снимки и останат материјал од видеонадзор. Од останатите тела кои што поседуваат бази на податоци а се користат во борбата против тероризмот ќе ги наброиме Visa Information System (VIS), чија што база содржи биометриски податоци кои, можеби не се екслузивно собрани со цел борба против тероризмот, но сепак придонесуваат во истата. Ист е случајот и со Schengen Information System (SIS I и SIS II) коишто содржат безброј податоци за лица кои се барани или непожелни во ЕУ (Kosevaliska, O., Ivanova, E. 2014). Овде можеме да ги наброиме и PNR (Passengers Name Records) датабазата која ја објаснуваме подолу во овој труд, како и Системот за електронска кривична евиденција ECRIS - European Criminal Records Information System; (Ѓуркова, О. 2011) и Eurodac (Регулатива бр. 2725/2000 на Советот од 11 декември 2000 година) која е база на отисоци од прсти односно дактилоскопски податоци од лица кои имаат аплицирано за азил или се илегални имигранти коишто се најдени на територијата на ЕУ; и Царинскиот информативен систем (CIS), коишто исто така имаат огромен придонес во размената на лични податоци во борбата против тероризмот.

---

[1] Напишано во забелешките на Бенџамин Франклин за Pennsylvania Assembly, објавено како: *Memoirs of the Life and Writings of Benjamin Franklin* (1818), www.archive.org/details/templefranklin02franrich.

[2] Самиот член 8 од Европската конвенција за заштита на човековите права, во ставот 1 го гарантира апсолутното право на приватен живот, додека во став 2 истото право го дерогира, но во конкретни ситуации.

Член 8 од ЕКЧП гласи:

Право на почитување на приватниот и семејниот живот

Секој човек има право на почитување на неговиот приватен и семеен живот, домот и преписката.

Јавната власт не смее да се меша во остварувањето на ова право, освен ако тоа мешање е предвидено со закон и ако претставува мерка која е во интерес на државната и јавната безбедност, економската благосостојба на земјата, заштитата на поредокот и спречувањето на кривични дела, заштитата на здравјето и моралот, или заштитата на правата и слободите на другите, во едно демократско општество. Секој исклучок од ова фундаментално право треба да биде определен рестриктивно.

Влијанието на 11 септември 2001 година врз европското законодавство за заштита на лични податоци

По терористичките напади на кулите близначки и Вашингтон во 2001 година, европската безбедносна политика стана една од хиперактивните области во креирање на нови политики во рамките на ЕУ-законодавството (Henderson, K. (Eds). 2005, стр.154). Овој настан сериозно влијаеше и на брзината во создавањето на нови форми на соработка меѓу ЕУ и САД. Иако целата оваа еуфорија не траеше долго, поради националната чувствителност кон мерките коишто требаше да се имплементираат во националното и европското законодавство, сепак можеме да констатираме дека брзината со која се имплементираа повеќето антитерористички мерки беше на завидно ниво. Она што претходно траеше со години, по нападите се реши за само 3 месеци. Причина за ова секако беше фактот што ниту еден политичар не сакаше да делува како „спор" во состојба на терористички закани. Терористичките напади докажаа и дека индивидуални држави не можат многу да помогнат во борбата против тероризмот и дека е неопходно вкрстување на информациите и податоците коишто меѓусебно ги имаат. Само две недели по нападите, Европскиот совет меѓу другите одлуки, одлучи и да ја стави во сила долго одложуваната соработка во размената на податоци помеѓу националните разузнавачки служби. Исто така, ЕУРОПОЛ доби специјална единица за борба против тероризмот и соработка со САД во ова поле (Segell, G. 2004, стр. 83–84). Соработката на ЕУ со САД во однос на преносот на лични податоци со цел успешна борба против тероризмот конечно стана реалност преку потпишување на договорот за соработка меѓу ЕУРОПОЛ и разузнавачките органи во САД (Dubois, D., 2002, стр.3). Европскиот совет одлучи да ја зајакне безбедноста на аеродромите, да го дополни законодавството врзано за перењето на пари и да се донесе гореспоменатата Одлука за замрзнување на имотот на лицата кои се осомничени за тероризам. Најзначајно беше прифаќањето на една општоприфатена дефиниција за тероризмот и стапувањето во сила на Европскиот налог за апсење. Последователно во казненото законодавство на сите земји членки на ЕУ, како и во останатите земји на Европа, беа инкриминирани тероризмот, неговото финансирање и членството во терористички организации. Во таа смисла Велика Британија ги зголеми надлежностите на полицијата во однос на претресот и апсењето на осомничените, замрзнувањето и конфискацијата на имотот и правото да ги задржи податоците за телефонските разговори и примената и испратената email пошта. Германија ја прошири надлежноста на надлежните органи во однос на пристапот до личните податоци давајќи им скоро одврзани раце во однос на таен мониторинг преку телефонските и електронските комуникации. Франција воведе нови мерки во борбата против тероризмот кои на надлежните органи им даваат поширок надлежности при следењето на комуникациите на осомничените лица, и сл. (Rees, W. 2006, стр.79-88).

Заштитата на лични податоци и националната безбедност во пракса со особен осврт на т.н. „црни листи"

Заштитата на лични податоци во пракса, логично, е многу поразлична од она што е наведено во многубројните правни инструменти коишто ја гарантираат истата.

Европскиот суд за човекови права е преплавен со случаи во кои граѓаните на ЕУ бараат заштита на приватноста како и затоа што истата им е прекршена (Council of Europe, 2009). Судот во Стразбур има донесено најмногу пресуди за прекршување на ова право од страна на истражните органи при спроведување на истраги во кои применуваат истражни дејства како прислушување на телефонските разговори на осомничени лица и нивен таен мониторинг.[3] Во

[3] Пресуда: Eur. Court HR, Klass and others v. Germany judgment of 6 September 1978, Series A no.28 (No violation of the Convention). Law authorising secret services to carry out secret monitoring of communications (postal and telephone;

Пресуда: Eur. Court HR, Malone v. The United Kingdom judgment of 2 August 1984, Series A no. 82 (Violation of Article 8 of the Convention). Interception of postal and telephone communications and release of information obtained from "metering" of telephones, both effected by or on behalf of the police within the general context of criminal investigation;

Пресуда: Eur. Court HR, Leander v. Sweden judgment of 26 March 1987, Series A no.116 (Violation of Articles 8, 10 and 13 of the Convention). Use of information kept in a secret police-register when assessing a person's suitability for employment on a post of importance for national security;

Пресуда: Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B (Violation of Article 8 of the Convention). Telephone tapping carried out by senior police officer under warrant issued by investigating judge;

Пресуда: Eur. Court HR, Lambert v. France judgment of 24 August 1998, Reports of Judgments and Decisions 1998-V (Violation of Article 8 of the Convention). Judgment whereby Court of Cassation refused a person locus standi to complain of interception of some of his telephone conversations, on the ground that it was a third party's line that had been tapped;

Пресуда: Eur. Court HR, Amann v. Switzerland judgment of 16 February 2000, application no. 27798/95 (Violation of Article 8 of the Convention). Recording a telephone conversation concerning business activities, and creation of a card index and storing of data, both by the Public Prosecutor; итн.

повеќето од овие пресуди е утврдено дека не станува збор за прекршување на правото коешто е гарантирано со член 8 од ЕКЧП.

Судска пракса по ова прашање има и Европскиот суд на правдата, испитувајќи ја легитимноста на некои од активностите на телата на ЕУ во заедничката надворешна и безбедносна политика. Во таа смисла во неколку пресуди судот одлучува за т.н. „црни листи" на можни терористи чијшто влез/излез од Унијата мора да биде строго мониториран (Sciroccо, A. (2008). Во таа смисла, во случаите Sison v. Council[4] и Organisation des Modjahedines de people d`Iran (OMPI) v. Council,[5] Судот во прв степен ги поништи двете одлуки на Советот со кои се имплементира член 2 став 3 од Регулативата (ЕС) No 2580/2001 за специфичните рестриктивни мерки упатени кон одредени личности и правни лица во случаите на борба против тероризмот. Овие тужители успеаја во спорот да бидат избришани од „црните листи". Во април 2007 година Советот одлучи да воведе нов начин според кој ќе се запишуваат физичките и правните лица на црната листа (Council press release 8425/07, стр. 34, 35 и Guild, E. 2008, стр.173-193. Со овие измени се обезбеди дека *засегнатите странки ќе бидат информирани дека Советот планира да ги стави или задржи на листата ... истите ќе бидат информирани преку „изјава за причините" која ќе ги содржи основите за вакватa одлука на Советот* (Council press release 8425/07 стр. 35). Советот, исто така, ќе ги „земе предвид сите реакции од засегнатите лица, пред да ја донесе својата конечна одлука за ставање на листата. "Оттука, државите членки се обврзани да обезбедат доволно податоци и основи за зацврснување на основите за ставање на лицата на листата.[6] За ова особено е важна и пресудата на Европскиот суд на правдата врзана за саудискиот бизнисмен Yassin Abdullah Kadi и меѓународната фондација Al Barakaat International Foundation, основана во Шведска, кои беа ставени на црната листа на ЕУ како финансиери на тероризмот. Одлуката за ова падна откако Кади успеа да докаже пред судот дека не бил информиран за замрзнувањето на неговиот имот, како и дека не му било дозволено правото на фер судење и правна заштита за да би можел да докаже дека тој не е поврзан со финансирање на тероризмот.

Во контекст на ова е неминовно накратко да елабориране за т.н. „црни листи" коишто содржат лични податоци за лица, групи или правни лица за кои постои (основано) сомнение дека се поврзани со терористички кривични дела односно нивно финансирање. Во таа смисла, личните податоци за овие лица – име, презиме, псевдоним, датум на раѓање, место на раѓање, број на пасош, како и членство во група или организација, се јавно видливи на „црната листа", во случај некој истите да ги препознае. Правна основа за ова има во Регулативата 2580/2011 од 27 декември 2001 година. Личните податоци на овие лица се наоѓаат во службениот весник на Унијата во контекст на претходно споменатата Регулатива. При додавање на нови лица на листата, на оваа Регулатива се додаваат амандмани во кои се наведени новите лица. Така на пример, едно од лицата кое се наоѓа на листата е опишано на следниот начин:

> *WALTERS, Jason Theodore James (a.k.a. Abdullah, a.k.a. David), роден на 6.3.1985 во Amersfoort (Холандија), пасош - холандски бр. NE8146378 – член на групата „Hofstadgroep".*[7]

Освен во службениот весник на Унијата овие податоци се присутни и на повеќе веб-сајтови кои ги имаат преземено овие податоци, основано, затоа што истите се и јавно прикажани во службениот весник со цел да бидат јавно достапни. Излишно би било да коментираме дали овде е прекршено правото на заштита на лични податоци кога како противтежа на истото се јавува борбата против тероризмот. Во овој случај борбата против тероризмот и неговото финансирање е далеку попретежна од заштитата на лични податоци. Но мора да се напомене дека во текот на целата постапка со која треба да се утврди дали едно лице е поврзано со терористички кривични дела или не, личните податоци мора да бидат заштитени и почитувани, бидејќи исходот од постапката може да биде и негативен а повредата позитивна. При утврдувањето на ова, неминовно е државите да разменат доволно лични податоци како со државните

---

[4] Пресуда: Case T-47/03 Sison v. Council, judgment of 11 July 2007;

[5] Пресуда: Case T-228/02, Organisation des Modjahedines de people d`Iran v. Council, [2006] ECR II-4665;

[6] Исто и во Case C-550/09, (Common foreign and security policy – Specific restrictive measures directed against certain persons and entities with a view to combating terrorism – Common Position 2001/931/CFSP – Regulation (EC) No 2580/2001 – Articles 2 and 3 – Inclusion of an organisation on the list of persons, groups and entities implicated in acts of terrorism – Transfer to an organisation, by members of that organisation, of funds originating from the collection of donations and the sale of publications) од 29 март 2010 година, достапна на сајтот http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d0f130d595f7170cf06a40539efdd03f56c51d57.e34KaxiLc3eQc40LaxqMbN4Oa3mLe0?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=84750&occ=first&dir=&cid=724684 , последен пат отворена на 30.10.2014 година.

[7] COUNCIL DECISION of 20 December 2007 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Decision 2007/445/EC, Сл.Весник на ЕУ L 340/100 од 22.12.2007, лице под реден број 35.

органи така и со приватните (на пр. банки кога станува збор за финансирање на тероризам).

Заштитата на личните податоци на патниците во PNR (**Passengers Name Record**)

Со оглед на фактот дека повеќето од терористичките напади се поврзани со авиопревозниците (дали преку киднапирање на авион или преку најбрз и најбезбеден начин на влез во државата која е цел на терористички напад) европското законодавство, по примерот на САД, содржи законски акти со кои се легализира преносот на лични податоци на патниците со цел сузбивање на тероризмот и обезбедување на националната безбедност.

По терористичките напади кои се случија во Мадрид во 2004 година, Советотпрво ја донесе Директивата 2004/82/ЕС, со која се утврди обврска кај превозниците да обезбедат пристап до личните податоци на патниците. Овој т.н. API (advanced passenger information) систем, ги вклучува следните лични податоци: име, презиме, датум на раѓање, број на пасош, националност и првичната точка на утовар на патникот. Превозниците можат да се соочат со минимална казна од 3000 евра во случај да не ги пренесат податоците за патник на граничната контрола на односната држава членка. Она што е врзано за заштитата на лични податоци во оваа Директива е одредбата од членот 6 според која *податоците за патниците ќе бидат избришани по истекот на 24 часа* ***освен во случаите кога овие лични податоци подоцна ќе им бидат потребни на надлежните органи...*** Уште повеќе загрижува фактот што директивата предвидува дека овие лични податоци можат да се користат од страна на државите членки за *цели основани со закон*. Што сè би можело овде законски да се оправда е речиси незамисливо. Употребата на личните податоци на патниците, првично за заштита на националната безбедност, донекаде може да има законска основа, но создавањето на плодна почва за нивна генерална употреба се коси со сите правни начела (Boehm, F. 2009, стр.11). Сметаме дека тоа што оваа Директива е донесена во несреќната околност (бомбардирањето на Мадрид) не може да оправда толку широка употреба на личните податоци. Буквалното „скенирање“ на личните податоци на секое лице коешто ќе одлучи да патува, поради можноста истото да биде терорист, звучи пресурово.

По донесувањето на оваа Директива, следуваа и PNR (Passengers Name records) договорите со САД, Канада и Австралија. Секако овие Договори се во името „на борбата против тероризмот, илегалната миграција како и сериозните закани за националната безбедност“. Во 2007 година Комисијата поднесе предлог за Рамковна одлука (Council Framework Decision on the use of Passenger name Record for law enforcement purposes COM, 2007) за употребата на PNR-податоците во случаи на спроведување на законот. Овој предлог беше мета на повеќе критики меѓу кои ќе го наведеме само мислењето на Европската агенција за заштита на човековите права FRA. Овој предлог, по влегувањето во сила на Лисабонскиот договор, се сметаше за застарен. Истиот, видоизменет, е сега дел од Стокхолмската програма.

Сметаме дека PNR-податоците (Исто и Hasbrouck, E.) се непотребно преопширни за целта за којашто служат. Истите содржат 19 различни лични податоци кои и не се нужни за да се евидентираат. Освен името, презимето, адресата на живеење, бројот на кредитната картичка, бројот на пасош и датум на негово издавање и рок на важење, број на виза, здравствено осигурување, IP-адресата, информации за контакт – број на мобилен, имејл, овие податоци содржат и податоци за исхраната на патникот (особено ова е начин да се индицира на припадник на муслиманската вероисповест, создавајќи овде и дискриминација) како и други чувствителни информации. Покрај ова проблематично е и прашањето за задолжителното внесување на податоци на лица кои не се патници, коишто лица би се контактирале во случај на несреќа. За нив се внесува име, презиме и место на живеење. Како главна причина поради која се бараат овие податоци секако се наведува обезбедување на националната безбедност (Thaker, J., 2012). Дискутабилно е чувањето на овие податоци. Имено, истите се чуваат во период од 30 дена по завршувањето на летот, потоа истите се анонимизираат и се чуваат 5 години во случај истите да им се потребни на истражните органи за спречување на тероризам и организиран криминал. Сметаме дека овој рок е несразмерно долг и се коси со гарантирањето на заштитата на лични податоци.

Иднината на заштитата на лични податоци во ЕУ

По терористичките напади од 11. 9. 2001 година, ЕУ безбедноста ја става секогаш пред слободите и правата на граѓаните. На мислење сме дека сè додека почитувањето на овие „вечни вредности“ на ЕУ не се усогласи, тогаш овие вредности се исклучуваат меѓусебно. Бидејќи оваа борба е на сметка на фундаменталните права, Унијата, мораше, во своите програми начелно да покаже дека ја зацврстува својата политика во почитувањето на овие права, предвидувајќи дела истите ќе ги унапредува постојано (Gutwirth, S.2012, стр.144).

Актуелната Стокхолмска програма[8] ја наследи Хашката програма, која важеше до 2009 година. Претседателството определи Програмата да се фокусира на обезбедување рамнотежа помеѓу безбедноста и заштитата на владеењето на правото и правата на човекот. Во таа смисла, во Програмата, од една страна, се подобрува полициската соработка, со тоа што се интензивира работата на ЕВРОПОЛ особено во размената на податоци во ЕУ. Од друга страна пак, во Програмата се предвидува зајакнување на правата на обвинетите во кривичната постапка, како и на правата на жртвите на криминалот и воедно подобрување на заштитата на податоците и приватноста.

Во глава 2.5. од Стокхолмската програма, е уредена заштита на правата на граѓаните во информатичкото општество. Во оваа глава е предвидено дека кога станува збор за оценување на приватноста на поединецот во областа на слобода, безбедност и правда, правото на слобода е најважно. Правото на приватност и правото на заштита на личните податоци се утврдени во Повелбата за фундаментални права. Сметаме дека Унијата мора да одговори на предизвикот од зголемувањето на размената на лични податоци и потребата да се обезбеди заштита на приватноста. Унијата мора да обезбеди сеопфатна стратегија за заштита на податоците и во рамките на Унијата и во нејзините односи со другите земји. Во тој контекст, треба да ја промовира примената на принципите утврдени во релевантните инструменти за заштита на податоците како што е Европската конвенција за заштита на поединците во однос на автоматска обработка на лични податоци од 1981 година. Исто така, мора да се предвиди и регулирање на околностите во кои мешањето на јавните власти во остварувањето на овие права ќе биде оправдано и строго контролирано.

ЕУ мора да биде подготвена да одговори на потребата за зголемена размена на лични податоци, истовремено обезбедувајќи и гарантирајќи ја почитта на заштита на истите. Европскиот совет е убеден дека технолошкиот развој не дава само нови предизвици за заштита на личните податоци, туку дека со технолошкиот развој се нудат нови можности за подобра заштита на лични податоци. На поширок фронт, ЕУ мора да биде движечка сила која стои зад развојот и унапредувањето на веќе постојните меѓународните стандарди за заштита на личните податоци и во склучување на нови соодветни билатерални или мултилатерални инструменти. Но при осмислувањето на новите мерките од ваков вид, треба да се земе предвид и влијанието што тие ќе го имаат на правото на приватност и правото на заштита на личните податоци на граѓаните.

Во Програмата се предвидени и посебни одредби кои се однесуваат на управување со проток на информации (Cools, M (eds.) 2010 стр.114-119). Европскиот совет со задоволство забележува дека развојот на настаните во ЕУ во текот на изминатите години доведе до широк избор на алатки за собирање, обработка и размена на информации помеѓу државните органи и другите европски тела во областа на слободата, безбедноста и правдата. Особено ова е за пофалба бидејќи се зголемува ефикасноста на принципот на достапност. Европскиот совет во Програмата, ја потврдува потребата за кохерентност и консолидација во развојот на управување и размена со информации и ги поканува Советот и Комисијата да „*ја спроведат Стратегијата за управување со информации во ЕУ за внатрешна безбедност која вклучува режим за заштита на податоците. Развојот мора да биде кохерентен со приоритетите утврдени во областа на слободата, безбедноста и правдата и внатрешната стратегија за безбедност, како и со законот, судската соработка, граничното управување и јавната заштита*“.[9] Во овој контекст, Европскиот совет ја поканува Комисијата да „ја оцени потребата за развој на модел на Европската размена на информации врз основа на процена на тековните инструменти, вклучувајќи ја и Одлуката на Советот 2008/615/ЈНА од 23 јуни 2008 година за прекуграничната соработка, особено во борбата против тероризмот и прекуграничниот криминал и Одлуката на Советот 2008/616/ ЈНА од 23 јуни 2008 година за спроведување на Одлуката 2008/615/ЈНА (Prüm) и Рамковната одлука на Советот 2006/960/ЈНА од 18 декември 2006 година за поедноставување на размената на информации и разузнавачки податоци меѓу органите на земјите членки на Европската Унија (т.н. „Шведска рамковна одлука”). „Со овие оцени ќе се утврди дали овие инструменти ја исполнуваат функцијата за која се наменети и дали ги исполнуваат целите на стратегијата за управување со податоци.

[8] Со Стокхолмската програма се определи работната рамка на ЕУ во областа на полициската и судската соработка за периодот од 2010-2014. Програмата официјално е усвоена на седница на Европскиот Советот на 10-11 декември 2009 година. Членовите на Европскиот парламент ја критикуваа нацрт-програмата во повеќе наврати, барајќи посеопфатен пристап кон прашањето за гарантирањето на процедуралните права и тврдејќи дека во Програмата е загубена пропорционалноста кога станува збор за примената на превентивни мерки. За ова види повеќе во списанието EUCRIM број 3, 2009 година, на European Criminal Law association Forum.

[9] Поглавје 4.2.2. од The Stockholm Programme — An Open And Secure Europe Serving And Protecting Citizens, Бр. 2010/C 115/01 објавена во Сл.Весник на ЕУ C 115/3 од 04.05.2010.

За да иднината на личните податоци се одвива на плодна почва, сметаме дека е неопходно земјите членки да гарантираат дека нивните приоритети, во рамките на националните програми за внатрешна стратегија за безбедност, ќе се приспособуваат на реалните потреби во заштитата на правото на приватност и заштита на личните податоци.

Квалитетот на европското законодавство несомнено треба да се подобри, но ова ќе биде без значење доколку истовремено не се подобри и неговата примена на национално ниво. Ова особено е очигледно од предлогот на Комисијата од јуни 2009 година, каде што таа упатува на „голема дупка" помеѓу правилата и политиките коишто се усвоени на национално ниво. Комисијата постојано упатува на фактот дека имплементацијата на правилата во националното право не претставува едноставен трансфер на правилата во домашното законодавство. Овие правила доживуваат многу евалуација и мониторинг кои круцијално ја променуваат целта на тие правила.

Покрај ова како сериозен проблем се јавува и т.н. EU acquis во областа на правдата и внатрешните работи (кој опфаќа приближно 1600 мерки). Овој преголем сет на правила многу придонесува во зголемувањето на и така постојниот проблем со имплементацијата.[10]

Заклучни согледувања и препораки

По нападите на кулите близначки во САД, дојде до драстична промена во начините на превенирање на тероризмот. Борбата против тероризмот стана опсесивна што резултира со перманентна контрола над животите на граѓаните и на податоците врзани со нив. Но, борбата против тероризмот и обезбедувањето на националната безбедност не смеат да се злоупотребуваат како основа за трансфер и обработка на личните податоци, затоа ЕУ е обврзана да ги штити своите граѓани од незаконско ракување со нивните лични податоци. Сметаме дека секоја од државите треба да обезбедува заштита на личните податоци на национално ниво, а ЕУ да го обезбеди ова на супранационално ниво.

По сето горенаведено, дискутирањето за заштита на личните податоци и националната безбедност стана многу комплицирано. Оваа тешкотија не е само од емоционална природа која не ни дозволува рамнодушно да ја ставиме заштитата пред безбедноста или обратно. Овој проблем е навистина суштествен и бара сериозна дебата. Ако категорично се определиме за приватноста тогаш се запрашуваме што ќе ни е приватност во услови на национален хаос и несигурност. Ако категорично се определиме за националната безбедност тогаш што ќе ни е да се чувствуваме безбедни кога сè за нашиот живот е општопознато. Тогаш што би било најдобро? Најдобро секако би било еден разумен баланс помеѓу двете засегнати категории, односно изнаоѓање на решение за обезбедување на националната безбедност со минимален притисок врз заштитата на личните податоци.

Дали граѓанинот ќе се одрече од ова право во прилог на националната безбедност? Друго прашање коешто треба да го имаме предвид е согласноста на субјектот на личните податоци. Во таа смисла, антитеристичките мерки вклучуваат собирање, употреба и пренос на лични податоци без притоа субјектот да е свесен за тоа, а уште помалку со негова согласност. Ова донекаде е и разбирливо затоа што тајноста на овие мерки е клучна за да истите вродат резултати заради кои и се применуваат. И од овде извира нов проблем. Субјектите не се свесни дека се собираат податоци за нив, не можат да дадат одговор кои податоци се точни а кои не. Податоците се собираат, споредуваат, ставаат во корелација со други податоци. Ова е плодна почва за креирање на нови податоци за субјектите за кои тие не се свесни.

Во никој случај не треба да се дозволи мерките на надзор да станат екстензивни во толкава мера што ја надминуваат и целта заради која се преземени. Преобемноста во собраните податоци не дава посигурен или поинаков резултат, туку само оди во прилог на прекршувањето на ова човеково право. Ова е типично при собирањето на личните податоци при примена на антитеристичките мерки. Надлежните органи како по правило, собираат повеќе лични податоци отколку што им се потребни за остварувањето на целта. Проблематична е и употребата на собраните податоци. Сметаме дека податоците треба да се користат само за целта за која се собрани. Во никој случај не треба податоците да се користат и за други (не) врзани случаи без за тоа да постои правен основ. Пожелно е субјектот на податоците да има сознание за ова доколку неговата информираност не ги загрозува целите на истрагата или не пречи на остварувањето на целта. Исто така не смее да се дозволи податоците да бидат пренесени на други органи на кои им се потребни за сосема друга цел.

За да се осигури заштитата на лични податоци потребно е и запазување на принципот на пропорционалност. Кога веќе зборуваме за пропорционалноста се запрашуваме дали е во ред да се истражува цела група на индивидуи со кои стапила во контакт една личност за која постои основано сомнение дека сторила или ќе стори кривично дело. Дали овде има

[10] Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen – Wider freedom in a safer environment, Commission Of The European Communities Brussels, COM (2009) 262/4.

пропорционалност? Зошто сите луѓе кои стапиле во контакт со осомниченият да бидат ставени под лупа?

Личните податоци кои се прибираат, обработуваат и пренесуваат во име на националната безбедност треба да бидат неопходни и релевантни за остварување на истата. Прекршувањето на горенаведеното или негово непочитување ја преминува границата поставена за да се заштитат личните податоци.

Користена литература:

Eijkman, Q., Schuurman, B. (2011): Preventive Counter-Terrorism and Non-Discrimination in the European Union: A Call for Systematic Evaluation , The International Centre for Counter Terrorism (ICCT) – The Hague, The Hague, June, стр. 9;

Кошевалиска, О., Нанев, Л. (2014): Информатичкиот систем на ЕВРОПОЛ, Меѓународна конференција, Еуробалкан, Скопје,

Кошевалиска, О., Иванова, Е. (2014): Шенгенски информациски систем, Меѓународна конференција, Еуробалкан, Скопје;

Tadjbakhsh, S., Chenoy, A. 2007: Human security: concepts and implications, Taylor & Francis, Political Science, стр. 123;

Busser, Els, 2009: : Data protection in EU and Us Criminal Cooperation: a substantive law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities, Maklu, стр. 53;

Pop, V.: MEPs Decry "Breach of Trust" in EU-US Data Deal', www.euobserver.com последен пристап 25.10.2014 година;

Ѓуркова, О. (2011): Заштитата на лични податоци во Системот за електоронска кривична евиденција на ЕУ (ECRIS) и македонското законодавство за заштита на лични податоци извадени од кривичната евиденција, Правник бр. 234, октомври 2011 година,

Регулатива бр. 2725/2000 на Советот од 11 декември 2000 година за основањето на Eurodac за споредба на отисоци од прсти за ефективна примена на Конвенцијата од Даблин, *Сл. весник ЕУ,* бр. L 316, 15.12.2000, срт. 1–10;

Henderson, K. (eds).: The Area of Freedom, Security and Justice in the Enlarged Europe, University of Leicester, Palgrave Macmillan Ltd 2005, стр.154;

Segell, G.: Intelligence Agency Relations between the European Union and the US, International Journal of Intelligence and Counter Intelligence, 17, 2004 година, стр. 83–84;

Dubois, D.: 'The Attacks of 11 September: EU-US Cooperation Against Terrorism in the Field of Justice and Home Affairs', European Foreign Affairs Review, 7, од 2002 година; стр.3;

Rees, W.: Transatlantic Counter-terrorism Cooperation, Routledge, Abingdon, Oxon, 2006, стр.79-88;

Европски суд за човекови права, Стразбур, официјален веб-сајт http://www.echr.coe.int ;

Council of Europe: Case Law Of The European Court Of Human Rights Concerning The Protection Of Personal Data, Dp (2009) Case Law, Strasbourg, March 2009, достапно на сајтот http://www.echr.coe.int ;

Пресуда: Eur. Court HR, Klass and others v. Germany judgment of 6 September 1978, Series A no.28 (No violation of the Convention). Law authorising secret services to carry out secret monitoring of communications (postal and telephone;

Пресуда: Eur. Court HR, Malone v. The United Kingdom judgment of 2 August 1984, Series A no. 82 (Violation of Article 8 of the Convention). Interception of postal and telephone communications and release of information obtained from "metering" of telephones, both effected by or on behalf of the police within the general context of criminal investigation;

Пресуда: Eur. Court HR, Leander v. Sweden judgment of 26 March 1987, Series A no.116 (Violation of Articles 8, 10 and 13 of the Convention). Use of information kept in a secret police-register when assessing a person's suitability for employment on a post of importance for national security;

Пресуда: Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B (Violation of Article 8 of the Convention). Telephone tapping carried out by senior police officer under warrant issued by investigating judge;

Пресуда: Eur. Court HR, Lambert v. France judgment of 24 August 1998, Reports of Judgments and Decisions 1998-V (Violation of Article 8 of the Convention). Judgment whereby Court of Cassation refused a person locus standi to complain of interception of some of his telephone conversations, on the ground that it was a third party's line that had been tapped;

Пресуда: Eur. Court HR, Amann v. Switzerland judgment of 16 February 2000, application no. 27798/95 (Violation of Article 8 of the Convention). Recording a telephone conversation concerning business activities, and creation of a card index and storing of data, both by the Public Prosecutor; итн.

Европски суд на правдата, Луксембург, официјален веб-сајт http://curia.europa.eu/jcms/jcms/Jo2_7047/ ;

Scirocco, A. (2008): 'The Lisbon Treaty and the Protection of Personal Data in the European Union' http://www.dataprotectionreview.eu/ пристап на 30.10.2014;.

Пресуда: Case T-47/03 Sison v. Council, judgment of 11 July 2007;

Пресуда: Case T-228/02, Organisation des Modjahedines de people d`Iran v. Council, [2006] ECR II-4665 ;
COUNCIL REGULATION (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, Official Journal of the European Communities L 344/70, 28.12.2001 година;
Council press release 8425/07 (Presse 80), стр. 34, 35 Guild, E. (2008): 'The Uses and Abuses of Counter-Terrorism Policies in Europe. The Case of the Terrorist Lists', Vol.46, No 1 Journal of Common Market Studies, 173-193;
COUNCIL DECISION of 20 December 2007 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealing Decision 2007/445/EC, Сл.Весник на ЕУ L 340/100 од 22.12.2007, лице под реден број 35;
Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data [2004] OJ L261/24 ;
Boehm, F. 2009: Confusing fundamental rights protection in Europe: Loopholes in Europe's fundamental rights protection exemplified on European data protection rules, Law Working Paper Series, Paper number 2009-01, University of Luxembourg, , стр.11;
Council Framework Decision on the use of Passenger name Record (PNR) for law enforcement purposes COM (2007) 654, on the use of Passenger Name Record (PNR) for law enforcement purposes in accordance with Article 4/2 of Regulation 168/2007 received on 18 September 2008 from the Presidency of the European Union;
Hasbrouck, E.: "What's in A Passenger Name Record (PNR)?," http://hasbrouck.org/articles/PNR.html последен пат отворена на 31.01.2013 година;
Thaker, J., 2012: API / PNR Regulatory Framework and Practical Applications, Seventh Symposium and Exhibition on ICAO and MRTDs, Biometrics and Security Standards 12-15 September 2011, Montreal;
Gutwirth, S.: European Data Protection: In Good Health?, Springer, Mar 31, 2012, стр.144;
EUCRIM број 3, 2009 година, на European Criminal Law association Forum;
The Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens, Бр. 2010/C 115/01 објавена во Сл. весник на ЕУ C 115/3 од 04.05.2010;
Cools, M (eds.) 2010: Eu and International Crime Control: Topical Issues (Governance of Security (Gofs) Research Paper Series, Vol. 4), Maklu, стр.114-119;
Gurkova, O., Ananiev, J. (2012): *National security versus protection of personal data in the EU*, Iustinianus Primus Law Review № 05, volume III, Winter 2012;
Buzarovska – Lazetik, G., Koshevaliska, O. (2013): Protection of personal data in criminal legislation in Macedonia vs. its protection in EU, Annals of the Bucharest University – The Law Series, Bucharest;
Kosevaliska, O. (2013): Protection on personal data when applying special investigative measures, „Правник", No. 259 Скопје;
Koshevaliska, O. (2013): Protection on personal data in criminal legislation in Macedonia, International scientific conference for the 20th Anniversary of the Constitution of the Russian Federation, Law Faculty in Kemerovo, Russia

Doz. Dr. Olga Koshevaliska, Juristische Fakultät, Universität „Goce Delchev", Stip

Die Achtung der grundlegenden Menschenrechte im Kampf gegen den Terrorismus

(Zusammenfassung)

Das Ziel des vorliegenden Beitrags ist es, einen kurzen Überblick über die europäische Gesetzgebung in Bezug auf das Thema zu geben, sowie den institutionellen Rahmen der Europäischen Union und ihrer Organe, die für die Bearbeitung personenbezogener Daten im Kampf gegen den Terrorismus zuständig sind, darzustellen. Dabei wird festgestellt, dass die erfolgreiche Terrorismusbekämpfung und die Erreichung eines hohen Maßes an nationaler Sicherheit ein wesentliches Ziel der EU ist. Um es zu erreichen, so wird weiter ausgeführt, ist jedoch erforderlich, in grundlegende Menschenrechte – das Recht auf Schutz der Privatsphäre und das Recht auf Schutz der personenbezogenen Daten – einzugreifen. Um diesen Konflikt zu lösen, müssen die Nutzung personenbezogener Daten und die Beschränkung des Rechts auf Privatsphäre rechtmäßig, ausdrücklich erlaubt und eine Ausnahme sein und durch eine zuständige Behörde überwacht werden. Besondere Aufmerkamkeit widmet der vorliegende Beitrag der Schaffung einer Politik zur Terrorismusbekämpfung nach den Terrorangriffen vom Jahr 2001 in den USA. Ein weiterer Schwerpunkt ist die Frage, inwiefern wir gewillt sind, unsere Rechte und Freiheiten zu opfern, um ein möglichst hohes Maß an nationale Sicherheit zu erreichen.

Schlüsselworte: Terrorismus, nationale Sicherheit, personenbezogene Daten, Recht auf Schutz der Privatsphäre, Europäische Union.